REMARKS

Applicants gratefully acknowledge the courtesy of the Examiner and Supervisory Patent Examiner Gilberto Barrón in granting an interview to Applicants' representative Sanford T. Colb, registration number 26,856, on 30 August 2004. In the interview, the Examiners and Applicants' representative discussed the Aboba reference, RFC 2194, Review of Roaming Implementations. Agreement was reached regarding an amendment of claim 1, as described below.

Applicants have carefully studied the outstanding Official Action. The present amendment is intended to be fully responsive to all points of rejection and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the present application are hereby respectfully requested.

Claims 1 - 3, 5 - 19, 33, and 35 - 43 are pending in the application.

Claims 7 - 8 stand objected to as depending from cancelled claim 4. Claim 7 has therefore been amended to depend from claim 1. Claim 8 depends from claim 7.

The objection to claims 7 - 8 is thereby deemed overcome.

Claims 1 - 3, 5 - 10, 12, 15 - 16, 19, 33, 36, 38, 40, and 42 - 43 stand rejected as being unpatentable over US Patent 6,385,729 to DiGiorgio et al. in view of US Patent 6,044,349 to Tolopka et al. and RFC 2194, Review of Roaming Implementations of Aboba et al.

DiGiorgio et al. describes a secure token device which provides a user with a vehicle for accessing services that are provided by an Internet Service Provider (ISP). The user places the token device in communication with a reader that is coupled to a computer system. The computer system includes a web browser for accessing the services provided by the ISP. The token device may perform an authentication protocol to authenticate itself to the ISP. The ISP may also be required to authenticate itself. The token device may hold an electronic currency token for payment of services rendered by the ISP. The token device may contain stored personal information about the user. The user may stipulate what portions of this personal information are provided to the ISP upon request.

Contextual information regarding sessions with the ISP may also be stored on the token device and used to restore a context of a previous session during a subsequent session.

Tolopka et al. describes a portable storage medium used to store data and provide access to information from an information dissemination system (IDS). The storage medium can store one or more location/key pairs. Each of the location/key pairs designates a particular IDS location as well as an access key to the particular IDS location. The storage medium can also store a plurality of information units. Levels of information categories can be individually accessed and categories of information units within levels can selectively be downloaded.

Aboba et al. describes roaming in IP environments. The ability to use any one of multiple Internet service providers (ISPs), while maintaining a formal, customer-vendor relationship with only one ISP is discussed.

Applicants are of the position that the rejection of claim 1 requires an additional reference, US Patent 6,055,637 of Hudson et al., cited by the Examiner in the Office Action mailed 4 December 2003 for the step of "identifying a local administrator...", as well as the Aboba et al. reference, for the step of "determining the local administrator".

Aboba et al., as discussed above, describes IP roaming, and therefore is not from a field of analogous art. Furthermore, Aboba et al. differs from the invention claimed in claim 1 because Aboba describes a Local ISP which does not administrate the roaming user. The local ISP serves as a conduit to locate and "make an authorization request to the user's Home ISP AAS for user ID and password verification. If the user is a valid user, the Home ISP authentication server sends a 'permission granted' message back to the Local ISP authentication server. The Local ISP authentication server then requests the NAS to grant the user a dynamic IP address from its address pool If the username or password is incorrect, the Home ISP AAS will send a rejection message to the Local ISP AAS, and the user will be dropped by the NAS." (Aboba et al. pgs. 6 - 7.)

In order to make clear the distinctions between the present invention, as claimed in claim 1, and the combination of DiGiorgio et al., Tolopka et al., Aboba et al., as well as Hudson et al., claim 1 has been amended as agreed

between the Examiner and Applicants' representative during the interview of 30 August 2004.

The amendment is supported, inter-alia, by page 18 of the specification.

Claim 1 is therefore deemed allowable.

Claims 2 - 3, 5 - 10, 12, 15 - 16, 19, and 42 - 43 depend, either directly or indirectly, from claim 1 and recite additional patentable subject matter.

Claims 2 - 3, 5 - 10, 12, 15 - 16, 19, and 42 - 43 are therefore deemed allowable.

Claim 33 is a system claim corresponding to claim 1 and has been correspondingly amended.

Amended claim 33 is therefore deemed allowable.

Claim 36 depends from claim 33 and recites additional patentable subject matter.

Claims 36 is therefore deemed allowable.

Claim 38 is a system claim in means-plus-function format, corresponding to claim 1, and has been correspondingly amended.

Amended claim 38 is therefore deemed allowable.

Claim 40 depends from claim 38 and recites additional patentable subject matter.

Claim 40 is therefore deemed allowable.

Claims 11, 18, 35, 37, 39 and 41 stand rejected under 35 USC 103(a) as being unpatentable over DiGiorgio et al., in view of Tolopka et al. and Aboba et. al, and further in view of US Patent 6,266,744 to Murphy et al.

Murphy et al. describes a method for authenticating a user over a network. The method includes an authentication module retrieving "authentication information from database 26" and storing in a smart card database at a remote location authentication information "by the same CA (Certified Authority) that issued the smart card to the user." (col. 6, lines 33 - 39).

Claims 11 and 18 depend from amended claim 1, and recite additional patentable subject matter.

Claims 11 and 18 are therefore deemed allowable.

Claims 35 and 37 depend, either directly or indirectly, from amended claim 33, and recite additional patentable subject matter.

Claims 35 and 37 are therefore deemed allowable.

Claims 39 and 41 depend, either directly or indirectly, from amended claim 38, and recite additional patentable subject matter.

Claims 39 and 41 are therefore deemed allowable.

Claims 13 and 14 stand rejected under 35 USC 103(a) as being unpatentable over DiGiorgio et al., in view of Tolopka et al. and Aboba et al., and further in view of US Patent 5,943,423 to Muftic et al.

Muftic et al. describes "a method of obtaining access to computer or network resources using a smart token, comprising: opening an application domain of a smart token used for access to a computer or a network; encrypting a password read from the application domain, so as to obtain an electronic password; sending a logon identification and the encrypted password to the computer or network for which access is desired; and verifying and validating as to whether the logon identification and the encrypted password are such that the access to the computer or network is permitted, wherein the step of sending a logon identification to the computer or network for which access is desired comprises: sending a user public key certificate stored on the smart token together with a user identification and a user random number to the computer or network; receiving from the computer or network the identity of the computer or network, a public key certificate of a target resource, a signed copy of the user random number and a second random number generated by the computer or network; verifying the signed copy of the user random number; and signing the second random number using the public key of the computer or network obtained from a certificate and returning the second random number with signature to the computer or network" (claim 1).

Claims 13 and 14 depend indirectly from amended claim 1, and recite additional patentable subject matter.

Claims 13 and 14 are therefore deemed allowable.

Claim 17 stands rejected under 35 USC 103 as being unpatentable over DiGiorgio et al., in view of Tolopka et al. and Aboba et al., and further in view of US Patent 5,838,812 to Pare, Jr. et al.

Pare, Jr. et al. describes "a tokenless identification system and method for authorization of transactions and transmissions is described. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously. The method and apparatus can be networked to act as a full or partial intermediary between other independent computer systems, or may be the sole computer systems carrying out all necessary executions."

Claim 17 depends indirectly from amended claim 1, and recites additional patentable subject matter.

Claim 17 is therefore deemed allowable.

In view of the foregoing remarks, it is respectfully submitted that the present application is now in condition for allowance. Favorable reconsideration and allowance of the present application are respectfully requested.

Respectfully submitted,

JULIAN COHEN
c/o LADAS & PARRY
26 WEST 61st STREET
NEW YORK, N. Y. 10023
Reg. No. 20302 (212) 708-1887